

2021 年 3 月 8 日

第 8 期

总第 481 期

2020 年度欧盟网络威胁态势报告

【译者按】2020 年 10 月，欧洲网络与信息安全局（ENISA）发布《欧盟网络威胁态势报告》，本报告是自 2013 年以来该组织第八年发布的系列报告。报告识别和评估了 2019 年 1 月至 2020 年 4 月欧盟及相关国家和地区面临的主要网络威胁态势、最易受攻击的行业和目标、网络攻击者情况、供网络攻击动机、常用技术等。报告通过分析年度网络攻击发展趋势，指出欧盟遭受网络威胁的复杂度有所提高，数字服务等五大行业最易遭受网络攻击。此外，报告还对 2019-2020 年欧盟国家网络威胁态势进行了具体分析，并提出展望建议。赛迪智库世界工业研究所对该报告进行了编译，期望对我国有关部门有所帮助。

【关键词】网络安全 网络攻击 欧盟

VISIT...

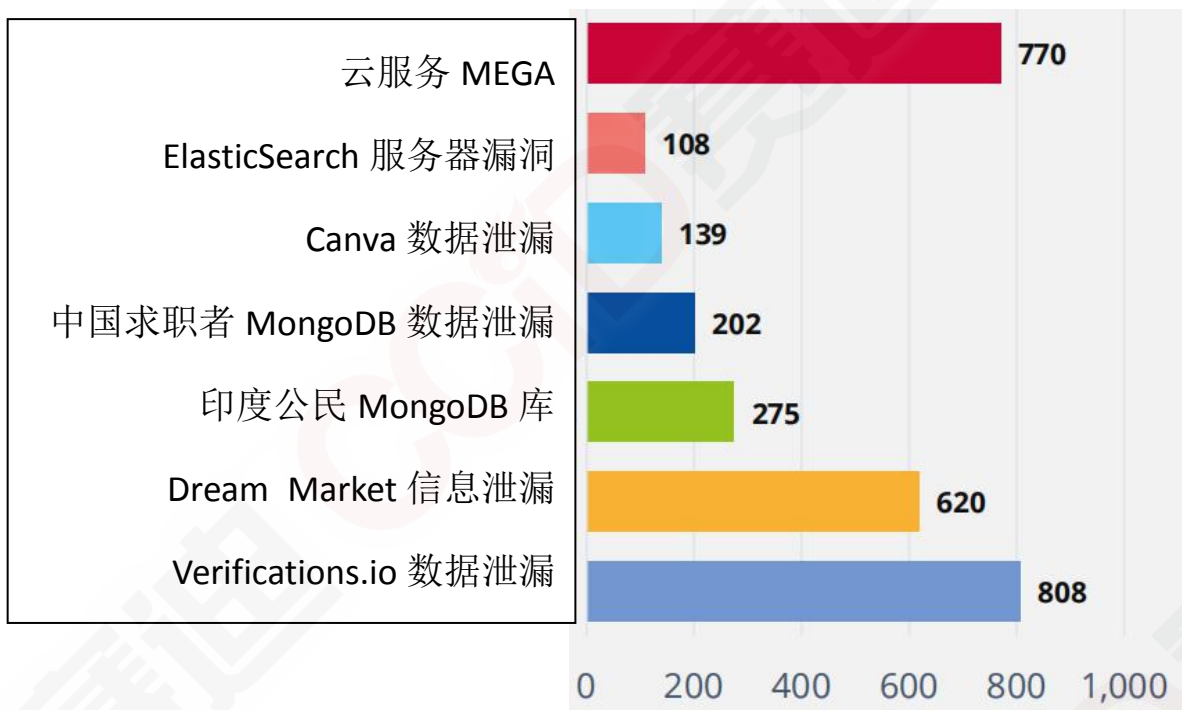
LANZAROTE
Caliente.COM

一、2019-2020 年欧盟网络威胁态势概述

（一）欧盟遭受网络威胁的复杂度有所提高

在过去的十年间，欧洲网络与信息安全局（ENISA）虽已将恶意软件列为前十五大威胁之一，但今年，我们发现仍有许多安全系统无法检测到这种威胁。恶意软件主要通过恶意的垃圾邮件进行传播，近年来又通过精心制作的网络钓鱼信息进行传播（图1）。

图 1：2019 年 1 月-2020 四月欧盟内数据泄露事件的分布



数据单位：百万条，数据来源：欧洲网络与信息安全局（ENISA）¹²³⁴⁵

因此，不论是科技公司还是电子邮件提供商，均开始将资金投入垃圾邮件过滤器以提高对恶意附件的检测能力。但是，攻击者也在不断“创新”，以增加接触潜在受害者的机会。在此期间，这些“创新”也给恶意参与者带来了非常高额的经济回报。尤其是在 2020 年，新冠疫情（COVID-19）给全球的医疗机构和从业

¹Elasticsearch：基于 Lucene 的搜索服务器，提供了一个分布式多用户能力的全文搜索引擎，使用 Java 语言开发，并作为 Apache 许可条款下的开放源码发布，是一种流行的企业级搜索引擎。Elasticsearch 用于云计算中，能够达到实时搜索，稳定，可靠，快速，安装使用方便。根据 DB-Engines 的排名显示，Elasticsearch 是最受欢迎的企业搜索引擎，其次是 Apache Solr，也是基于 Lucene。

² MongoDB：基于分布式文件存储的数据库。由 C++ 语言编写。旨在为 WEB 应用提供可扩展的高性能数据存储解决方案。

³ Dream Market：曾是全球最大的暗网市场，现已关闭。

⁴ Canva 数据库：知名在线设计软件数据库。

⁵ Verifications.io：总部位于美国的电子邮件验证公司。

人员带来了压力，而卫生行业也已成为防止网络攻击的最关键行业之一。针对医疗保健行业的勒索软件事件数量已经很多，在疫情期间依然有所增加。

欧洲网络与信息安全局（ENISA）梳理了欧盟及相关经济体 2019 年 1 月至 2020 年 4 月的重大网络攻击事件，包括：

2019 年 1 月，新西兰 MEGA 云数据泄漏，曝光了 7.7 亿封邮件和 2100 万个密码；

2019 年 2 月，美国 Verification.io 曝光了大约 8 亿条用户数据记录；

2019 年 3 月，挪威海德鲁遭受勒索软件攻击；

2019 年 4 月，美国脸书公司报告数据泄漏导致 5.4 亿条用户记录在公开服务器上曝光；

2019 年 5 月，德国蒂森克虏伯和拜耳遭到间谍恶意软件攻击；

2019 年 6 月，罗马尼亚 5 家医院遭到勒索软件 Badrabbit⁶的攻击；

2019 年 7 月，南非 City Power 电力公司遭到勒索软件攻击，导致约翰内斯堡供电中断；

2019 年 8 月，保加利亚个人所得税务局遭受数据泄漏，曝光

⁶ 新型勒索病毒“Bad Rabbit”2019 年曾在欧洲部分地区爆发，俄罗斯、乌克兰、土耳其、德国受到影响。据国内网络安全企业介绍，该病毒伪装成 Adobe flash player 欺骗用户安装，感染后会在局域网内扩散。该病毒在国内并无活跃迹象。

了所有成年公民的个人身份信息；

2019 年 9 月，万事达遭受数据泄漏，涉及欧洲大约 9 万个客户；

2019 年 10 月，格鲁吉亚多家网站和国家电视和电台广播公司遭受网络攻击；

2019 年 11 月，意大利裕信银行遭受数据泄漏，泄漏 300 万条记录；

2019 年 12 月，西班牙保赛固公司⁷遭到勒索软件攻击，导致运营停止；

2020 年 1 月，奥地利外交部遭受网络攻击；

2020 年 2 月，克罗地亚 INA 集团⁸遭到勒索软件攻击；

2020 年 3 月，总部位于比利时的欧洲电网遭黑客入；

2020 年 4 月，超过 50 万个 Zoom 账户信息在暗网出售。

综上所述，2019-2020 年欧盟及其相关地区遭受网络威胁的复杂度有所提高，不少攻击者会利用安全漏洞窃取证书进行攻击复合手段的网络攻击，导致数据泄露事件的数量居高不下，被窃取的财务信息和用户证书数量不断增加。在合理时间内，若可能影响正在使用的软件或库的已知漏洞没有被及时修补，则会产生严重后果。

⁷ 西班牙最大安保公司，成立于 1976 年，总部位于马德里，全球拥有雇员约 15 万人。

⁸ 克罗地亚 INA 集团是克罗地亚最大的石油工业集团之一。

（二）欧盟经济体内五大行业最易遭受网络攻击

通过分析统计期内遭受的攻击发现，欧盟最容易遭受网络攻击的行业包括数字服务、政府管理和技术行业等。其中，对数字服务提供商的攻击通常是通过充当代理以接触到其他更有吸引力的目标。对攻击技术行业的攻击方式通常是破坏供应链或寻找可资利用的漏洞。

在云服务方面，由于 MongoDB 数据库未受保护，与其关联的电子邮件平台 Verifications.io 遭受了重大数据泄露，导致包括个人身份信息等敏感信息的超 8 亿封电子邮件信息曝光。另如，一个受欢迎的黑客论坛上曾曝光了云服务商 MEGA⁹ 上超过 7.7 亿个电子邮件地址和 2100 万个唯一密码，成为历史上最重要的违反个人证书的集合，称为“集合 1”。再如，云和虚拟化提供商 Citrix 受到了有针对性的网络攻击，攻击者采用了被称为“密码喷雾”的技术破解了关键软件漏洞。此外，云托管提供商 iNSYNQ 遭遇的勒索软件攻击导致客户无法访问数据，持续时间超过一周，迫使客户只得依赖本地备份完成业务。

在数字化服务方面，电子邮件、社交平台 and 在线协作平台等服务提供商在 2019 年也受到了攻击，上述服务还被用作进一步攻击的代理工具，引发更大后果。

⁹ Mega: 网络存储服务商。据报道,大约有 1.2 万个文件,总计 87GB 的数据于 2019 年从 MEGA 被泄露。

在政府管理方面，一些政府愿意支付给黑客高昂赎金，这给一些网络不法分子带来巨大经济收益，因此正在使公共部门成为最具吸引力的勒索软件攻击目标之一。

在科技行业，2019 年受到的攻击主要集中在对供应链的攻击，攻击者试图通过零日漏洞和后门攻击破坏软件开发。

在金融行业，报告期内与金融组织有关的事件数大幅增加。在卫生保健行业，对卫生保健行业的攻击数量也在持续增长。

二、2019-2020 年欧盟国家网络威胁态势具体情况分析

（一）主要趋势

2019-2020 年，84 % 的网络攻击依赖于社交软件，67 % 的恶意软件是通过加密的 HTTPS 连接发送的，每天都有 230000 种新恶意软件出现，受攻击者平均需要 6 个月才能检测到数据泄露，71 % 的组织经历过恶意软件活动，基本上都是从一名员工传播到另一名员工。全球木马活动活跃，其中 Emotet 和 Agent Tesla 是最常见和最危险的恶意软件。

网络钓鱼仍然是传播恶意工具最成功的技术之一。强大的网络钓鱼诱饵包括电话诈骗、虚假发票、付款、报价以及购买和销售订单。

勒索软件继续为恶意行为者带来可观的经济收益。最近开展

的一项研究发现了人为操控的勒索软件活动，在此类活动中，攻击者采用了传统上与有针对性的攻击（例如来自民族国家行为者的攻击）相关联的证书盗窃和内网漫游方法。

除上述两项之外，由于在线购物者数量的不断增加，从 2019 年至 2020 年，信用卡遭遇侧录盗窃的威胁越来越大；由于大量的证书和个人信息遭到窃取，商务电子邮件诈骗成为一个日益严重的威胁。

（二）活跃的网络攻击者情况

确定哪些人和组织应该为网络安全事件负责，或者将责任归咎于哪个个人或团体，是一项非常艰巨的任务。但是，从威胁情报的角度来看，有必要对此类行为进行分类，了解特定攻击者的动态和操作方式。通过这种分析，通常有助于防御者寻找特定的路径，并尝试预测下一次攻击行动。例如，拉撒路集团（Lazarus Group）是臭名昭著的高级持续性威胁（APT）团体，在本报告所述期间，该团体在经济和间谍活动攻击方面均比较活跃。多起事件都与该团体有关，包括针对加密货币交易平台用户及其系统的 Applejeus 行动，此外，被认为是该团体所为的主要事件包括：

（1）2019 年 11 月，入侵印度一家核电厂和太空研究组织；

（2）2019 年 10 月破坏针对交易所管理员的加密货币交易应用程序；

(3) 2019 年 9 月，攻击印度多家自动柜员机（ATM）和银行；

(4) 2019 年 8 月，通过 Google Play 商店中的木马化应用程序定位韩国的安卓（Android）用户。

其他值得警惕的活跃网络攻击者（组织）包括：

(1) TURLA：2019 年，该组织将 40 多个国家的教育、政府、军事、研究和制药部门的微软 Exchange 电子邮件服务器作为攻击目标。

(2) APT27：该组织破坏了中东两个国家政府机构的 SharePoint 服务器。

(3) VICIOUS PANDA：2020 年 4 月，针对蒙古国公共行政当局的行为是该组织所为。

(4) GAMAREDON：该组织从 2019 年 12 月开始发起了针对乌克兰国防部的鱼叉式网络钓鱼行动。

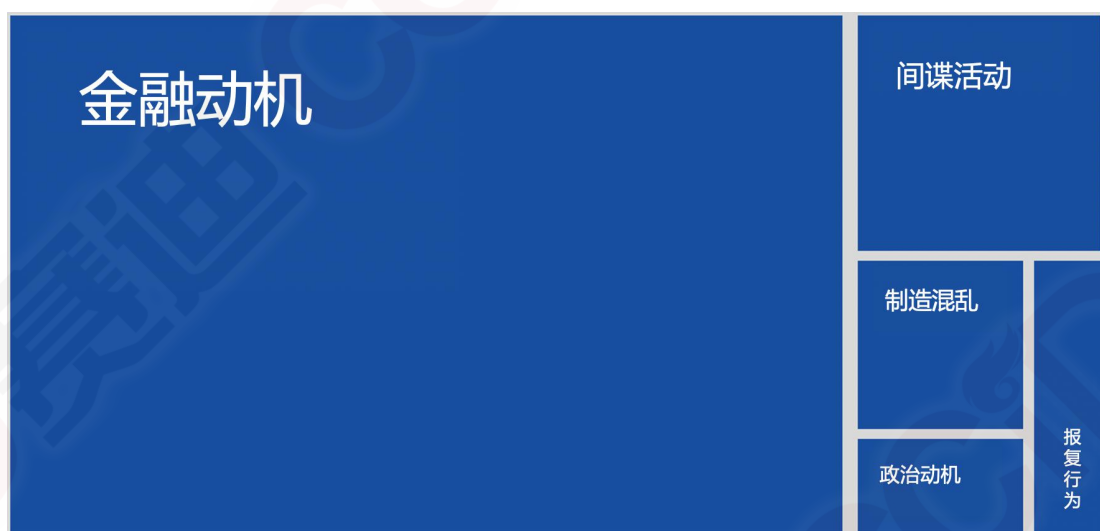
上述网络攻击中，60%是有组织的犯罪，16%属于国家行政系统攻击，10%是内部人员攻击，8%属于系统管理员攻击，4%是终端用户攻击。

（三）攻击动机分析

虽然很难确定网络攻击背后的主要动机，但我们仍然可以根据事件的结果对其进行分类。在某些情况下，可以在一次攻击中

识别出多种动机。例如，间谍活动、政治因素、金融因素和制造混乱往往是混合在一起的，很多网络攻击事件的漏洞源于自动化系统，并以“软件即服务”的模式传播，以加密货币支付。这些服务包括分发勒索软件、命令和控制（C2）、分布式拒绝服务（DDoS）、垃圾邮件和其他非法活动。

图 2：常见的五大网络攻击动机



数据来源：欧洲网络与信息安全局（ENISA）

归纳而言，网络攻击主要有五个主要动机：金融因素、间谍活动、制造混乱、政治因素和报复行为。以下仅对金融因素和间谍活动进行阐述。

金融因素动机是在本报告期内造成信息、数据和用户证书遭盗用的事件数量是最多的。在大多数情况下，其目的是窃取数据或信息并在暗网上出售。还可以确定这些信息或数据的其他用途，以实现间谍活动或金融欺诈等其他类型的攻击，产生完全不

同的结果。例如，某组织从 16 个遭黑客攻击的网站上窃取了超 6.2 亿个账户的信息，并在颇受欢迎的暗网市场 Dream Market 上出售。

间谍活动引发的网络攻击在报告期内不断增加，主要是因为持续的地缘政治和商业紧张局势。此类事件的数量并不多，但事件的规模和严重程度在 ENISA 列出的 5 大动机中名列第二。法新社（Agence France Presse）报道称，空客公司成为一场复杂的网络间谍活动的受害者，攻击者侵入了几家空客公司供应商的 IT 系统，并从那里侵入了该公司的 IT 系统。

（四）常用攻击技术

网络攻击平均需要三个步骤来获取受害者的宝贵资产。在审查最常用的攻击载体时，我们必须分清切入点、行动过程和对资产采取行动的优先级。了解这些关键步骤有助于制定防御策略。

报告得出，2019-2020 年，最常用来发起网络攻击的技术步骤包括利用窃取的证书进行安装恶意软件暴力破解、社交网络、配置错误和利用 web 应用程序。安装恶意软件是被广泛使用的网络攻击技术，一旦安装成功，它就可以为攻击者进行网络侦察，在受害者的系统和网络中移动，安装勒索软件等其他工具，窃取数据并与 C2 服务器通信。利用社交网络来策划攻击则是借助了网络钓鱼和商务电子邮件诈骗（BEC）等工具。web 应用程序经

常被当作一个切入点，因为人们越来越多地采用这种类型的应用程序将数据传输到云，大量事件也表明，云配置中的错误和系统的误用是必不可少的切入点。此外，其他不经常使用但同样重要的手段包括利用漏洞和软件后门，这些手段通常用于更复杂更高级的攻击。

（五）最易受攻击的五大目标

报告发现，网络攻击者最希望得到五种类型的资产。一是工业产权和商业秘密，这是攻击者最想得到的资产，因为这些资产具有很高的价值。二是国家机密或军事机密信息，这类资产包括国家认为敏感的所有信息，尤其在 2019 年，国家之间的贸易和外交紧张局势使得这类信息更具吸引力。三是服务器基础架构，这是非数据的敏感资产，且很多攻击就是为了接管受害者的服务器基础架构。四是真实数据，数据是可产生利润的宝贵资产，也是发起攻击要实现的目标。五是财务数据，诸如信用卡、银行和付款信息等财务数据的价值始终吸引着网络罪犯。

三、未来展望和建议

该部分主要展望新冠疫情给未来欧盟网络威胁态势带来何种变化。

欧洲网络与信息安全局（ENISA）绘制了 2019-2020 年欧盟

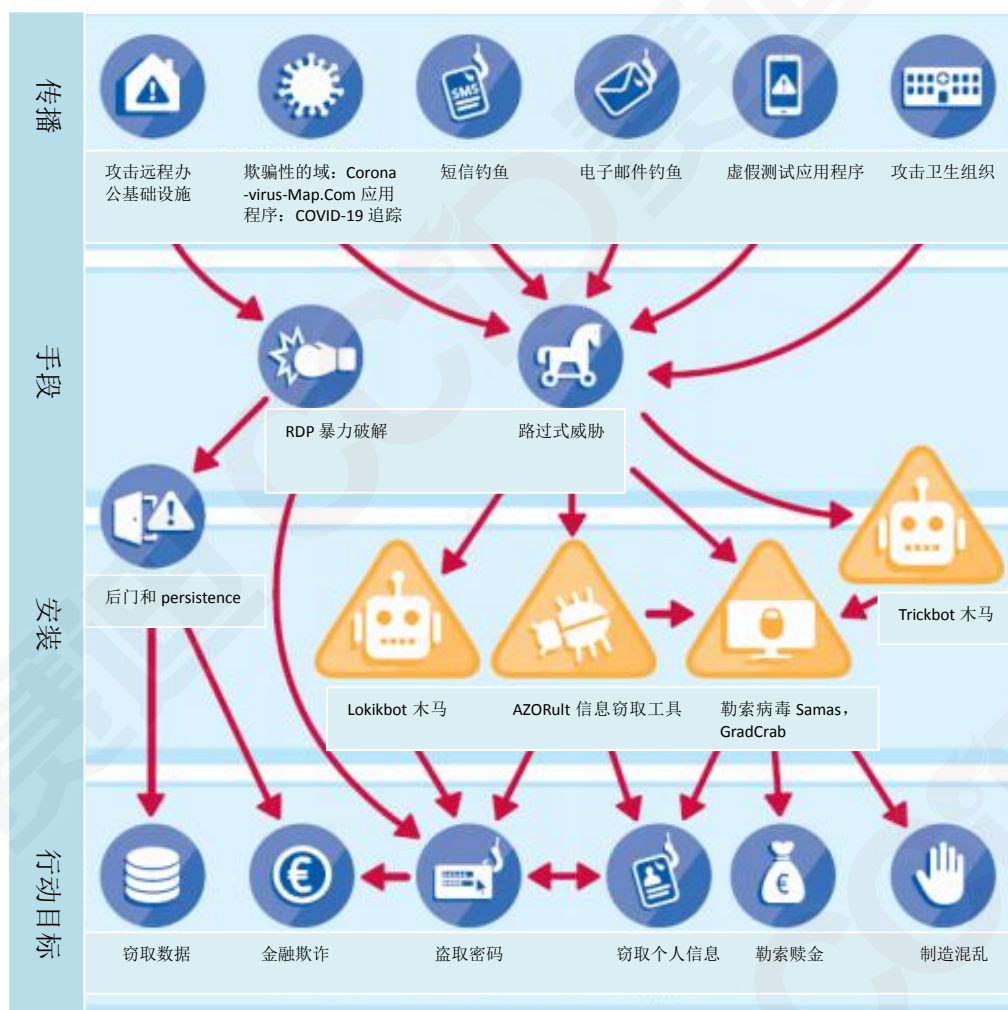
网络威胁态势图（图 3），帮助决策者和政策制定者制定战略，保护公民、组织和网络空间。需要说明的是，这项工作是欧洲网络与信息安全局的战略组成部分，并会为 ENISA 的利益相关者提供战略情报。应欧盟委员会和成员国的要求，下年度中心主题是下一代移动通信（5G）和人工智能对网络安全的威胁。

报告认为，新冠疫情期间将成为网络攻击恶意行为的多发时期，攻击者可能会加大对远程工作、在线购物和电子医疗等敏感领域进行攻击，医疗保健服务提供商、居家办公的员工是他们的易攻击对象。

例如，捷克共和国布尔诺大学医院（Brno University Hospital）在新冠疫情期间就已经遭到了网络攻击，使得病人的就医路线被迫改变并推迟了手术，由于该医院是捷克共和国最大的新冠病毒检测实验室之一，因此可将该事件认定为严重事件。

为此，欧洲网络与信息安全局（ENISA）将发起提高公众网络安全意识的活动，相关将资源分享给网络安全专家。

图 3 2019-2020 年欧盟网络威胁态势图



数据来源：欧洲网络与信息安全局（ENISA）

总的来说，新冠疫情期间网络攻击的传播将会围绕远程办公设施、与新冠疫情相关的欺骗性程序、虚假测试程序、短信钓鱼、电子邮件钓鱼展开，手段主要是暴力破解、后门、木马、信息窃取工具等，行动目标是窃取数据、金融欺诈、窃取密码、窃取个人信息、勒索赎金、制造混乱等。

新冠疫情期间欧盟将面临的更为复杂严峻的网络威胁和网

络安全挑战。

译自：*From January 2019 to April 2020 Main Incidents in the EU and Worldwide ENISA Threat Landscape, Oct.2020, European Union Agency for Network and Information Security (ENISA)*

译文作者：世界工业研究所 王哲

联系方式：13126598700

电子邮件：wangzhe@ccidthinktank.com

赛迪智库

面向政府 服务决策

咨询翘楚在这里汇聚

规划研究所

工业经济研究所

电子信息研究所

集成电路研究所

产业政策研究所

科技与标准研究所

知识产权研究所

世界工业研究所

无线电管理研究所

信息化与软件产业研究所

军民融合研究所

政策法规研究所

安全产业研究所

网络安全研究所

中小企业研究所

节能与环保研究所

材料工业研究所

消费品工业研究所

编辑部：工业和信息化部赛迪研究院

通讯地址：北京市海淀区万寿路27号院8号楼12层

邮政编码：100846

联系人：王 乐

联系电话：010-68200552 13701083941

传 真：010-68209616

网 址：www.ccidwise.com

电子邮件：wangle@ccidgroup.com

报：部领导

送：部机关各司局，各地方工业和信息化主管部门，
相关部门及研究单位，相关行业协会

编辑部：赛迪工业和信息化研究院

通讯地址：北京市海淀区紫竹院路 66 号赛迪大厦 15 层国际合作处

邮政编码：100048

联系人：袁素雅

联系电话：（010）88559543 13263204219

传 真：（010）88558833

网 址：www.ccidgroup.com

电子邮件：yuansy@ccidtrans.com

